Privacy impact Assessment voor het wetsontwerp Computercriminaliteit III

Den Haag, 7 januari 2014

Vooraf

Deze bijlage hoort bij de memorie van toelichting bij het wetsvoorstel Computercriminaliteit III. Het bevat de antwoorden op de vragen zoals die zijn gesteld in het toetsmodel Privacy Impact Assessment Rijksdienst (kamerstukken II 2012-2013, 26643, nr. 282 herdruk 1).

Wat beoogt het wetsvoorstel?

Dit wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken. Het wetsvoorstel vormt een uitwerking van eerdere toezeggingen aan de Tweede Kamer alsmede van het in het regeerakkoord van dit kabinet opgenomen voornemen om de toenemende bedreigingen en kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden. Het wetsvoorstel stelt voor het juridisch instrumentarium aan te passen naar aanleiding van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie (Bruggen slaan, Regeerakkoord VVD – PvdA, 29 oktober 2012, blz. 28). Voorgesteld wordt te komen tot uitbreiding van de strafvorderlijke bevoegdheden en van een aantal strafbepalingen.

Wat wordt voorgesteld?

In de eerste plaats wordt voorgesteld een nieuwe bevoegdheid te creëren voor daartoe aangewezen opsporingsambtenaren om een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Daarbij kan de beveiliging worden doorbroken of kunnen technische handelingen worden verricht om toegang te verschaffen tot het geautomatiseerde werk. Ook kan heimelijk software worden geïnstalleerd met behulp waarvan op specifieke punten de beveiliging wordt doorbroken of omzeild en waarmee de versleuteling van gegevens ongedaan kan worden gemaakt. In dit verband wordt tevens voorgesteld de omschrijving van het begrip 'geautomatiseerd werk' aan te passen, mede in het licht van de Europese regelgeving.

In de tweede plaats wordt voorgesteld om de regeling van de bevoegdheid van de officier van justitie aan te passen om, met machtiging van de rechter-commissaris, te bevelen dat gegevens op internet ontoegankelijk worden gemaakt. Dit is thans geregeld in artikel 54a van het Wetboek van Strafrecht. De voorgestelde wijziging heeft ten doel te komen tot een betere uitvoering van de huidige wet. Het betreft het beter beschermen van de samenleving tegen strafbare feiten die op internet worden begaan. In de derde plaats wordt voorgesteld een wettelijke bevoegdheid te creëren tot het geven van een bevel aan een verdachte tot het toegankelijk maken van versleutelde elektronische gegevens (hierna ook te noemen: decryptiebevel). Met de wettelijke regeling van het decryptiebevel aan de verdachte wordt het juridisch instrumentarium van politie en justitie om toegang te kunnen verkrijgen tot versleutelde gegevens, aangepast aan de eisen van deze tijd in verband met de opsporing van enkele ernstige strafbare feiten en de waarheidsvinding. Mede in het licht van de eisen van artikel 6 EVRM wordt de uitoefening beperkt tot het maken van een beroep of gewoonte van de vervaardiging, verspreiding en het bezit van kinderpornografie (artikel 240b, tweede lid, Sr) en het plegen van terroristische misdrijven waarop een gevangenisstraf van 8 jaar of meer is gesteld.

In de vierde plaats wordt voorgesteld het wederrechtelijk overnemen van gegevens en het voorhanden hebben of bekend maken van door misdrijf verkregen gegevens strafbaar te stellen. Daardoor worden gedragingen strafbaar die kunnen worden beschouwd als "heling" van gegevens. Hiermee wordt in een betere strafrechtelijke bescherming van computergegevens voorzien.

In de vijfde plaats wordt voorgesteld de strafbaarstelling van het corrumperen van minderjarigen en grooming (artikelen 248d en 248e Sr) te verruimen. Met de term grooming wordt gedoeld op het ongewenst benaderen van kinderen op het internet, bijvoorbeeld in chatrooms, met het oogmerk om hen tot seksueel misbruik te verleiden. Om dit maatschappelijk zeer schadelijke verschijnsel beter te kunnen bestrijden is het wenselijk opsporingsambtenaren in te zetten ('lokpubers') die zich als een minderjarige voordoen. Daarvoor is nodig dat de strafbaarheid zich ook richt op de situatie waarin de verdachte ten onrechte aanneemt dat hij met een minderjarige van doen heeft.

In de zesde plaats wordt voorgesteld de zogenaamde online handelsfraude strafbaar te stellen. Met deze term wordt gedoeld op het via het internet aanbieden van goederen of diensten, zonder de intentie die goederen of diensten te leveren, zodat de kopers worden gedupeerd. Zodra de koper merkt dat hij is bedrogen is de website doorgaans uit de lucht gehaald en is de verkoper niet meer te achterhalen. Het voorstel biedt de mogelijkheid strafrechtelijk op te treden tegen personen die een beroep of gewoonte maken van het aanbieden van goederen of diensten op het internet, zonder de intentie om die goederen of diensten daadwerkelijk te leveren. Dit onderdeel van het wetsvoorstel valt niet binnen het bereik van de voorwaarden dat het onderdeel dient uit te maken van de PIA.

Tenslotte zijn in dit wetsvoorstel enkele wijzigingen van meer technische aard opgenomen, waarmee eerdere omissies worden hersteld.

De PIA richt zich op het nieuwe artikel 125ja van het Wetboek van Strafvordering. Alleen in dit artikel uit het wetsvoorstel is sprake van het verwerken van persoonsgegevens in databestanden als bedoeld in het toetsmodel.

Nieuw artikel in het Wetboek van Strafvordering

Doorzoeking ter vastlegging van gegevens en onderzoek in een geautomatiseerd werk

Artikel 125ja, eerste lid

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager, bij de verdachte in gebruik, en met een technisch hulpmiddel onderzoek doet met het oog op:

a. het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker;

b. het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn verwerkt, of die eerst na het tijdstip van afgifte van het bevel worden verwerkt, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;

c. de ontoegankelijkmaking van gegevens;

d. een bevel als bedoeld in de artikelen 126l, 126m, 126s, 126t, 126zf of 126zg;

e. een bevel als bedoeld in de artikelen 126g, 126o of 126zd, eerste lid, onder a.

In het belang van het onderzoek kunnen gegevens worden vastgelegd. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.

I. Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/gegevensminimalisering

1. Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?

Ja. Bij het onderzoek in een geautomatiseerd werk door daartoe aangewezen opsporingsambtenaren zal bij het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker toegang verkregen worden tot de persoonsgegevens van de gebruiker. Deze gegevens kunnen in het geautomatiseerd werk zelf aanwezig c.q. via het geautomatiseerde werk bereikbaar zijn. Ook kunnen voorafgaand aan het binnendringen in het geautomatiseerde werk, persoonsgegevens en andere gegevens verwerkt worden ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven. Deze gegevens kunnen ertoe bijdragen de opsporingsambtenaar in staat te stellen om het geautomatiseerde werk binnen te dringen. Dit betreft naast gegevens van meer technische aard over de gebruikte geautomatiseerde systemen, ook gegevens over geïdentificeerde of identificeerbare personen.

Verder kan er sprake zijn van het overnemen van persoonsgegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn verwerkt, of die eerst na het tijdstip van afgifte van het bevel worden verwerkt, voor zover redelijkerwijs nodig voor de waarheidsvinding. Voorts kunnen gegevens waaronder persoonsgegevens op afstand ontoegankelijk worden gemaakt, c.q. verwijderd vanuit het geautomatiseerde systeem. De gegevens kunnen ook bijzondere persoonsgegevens bevatten. Conform artikel 1 onder a van de Wet politiegegevens (Wpg) is een gegeven elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt. Dit geldt dus ook bij de uitoefening van de bevoegdheid onder artikel 125ja van het Wetboek van Strafvordering.

2. Andere specifieke persoonsgegevens?

2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?

De persoonsgegevens worden verzameld en verwerkt ten behoeve van de opsporing van ernstige misdrijven. Het is niet de bedoeling gegevens te verwerken over de financiële of economische situatie van de betrokkene, anders dan met het oog op de opsporing van ernstige strafbare feiten. Niet uitgesloten is dat gegevens over de financiële of economische situatie van betrokkenen deel uitmaken van de politiegegevens die via het onderzoek in een geautomatiseerd werk worden verkregen. Als deze politiegegevens onderdeel gaan uitmaken van de processtukken in een strafzaak, waaronder de dagvaarding, dan dienen zij de bewijsvoering en zijn niet gericht op stigmatisering of uitsluiting.

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?

De persoonsgegevens worden verzameld en verwerkt ten behoeve van de opsporing van ernstige misdrijven. Het is niet de bedoeling gegevens te verwerken over kwetsbare groepen of personen,

anders dan met het oog op de opsporing van ernstige strafbare feiten. Niet uitgesloten is dat gegevens over kwetsbare groepen of personen deel uitmaken van politiegegevens die via het onderzoek in een geautomatiseerd werk worden verkregen. In artikel 5 van de Wet politiegegevens worden specifieke regels gegeven over de verwerking van dergelijke gegevens ten behoeve van de uitvoering van de politietaak.

2c.Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?
Ja. Het onderzoek in een geautomatiseerd werk kan zijn gericht op het verzamelen en verwerken van gebruikersnamen, wachtwoorden en andere inloggegevens, ten behoeve van de opsporing van ernstige misdrijven.

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?

De persoonsgegevens worden verzameld en verwerkt ten behoeve van de opsporing van ernstige misdrijven. Het is niet de bedoeling biometrische gegevens te verwerken, anders dan met het oog op de opsporing van ernstige strafbare feiten. Niet uitgesloten is dat metrische gegevens kunnen deel uitmaken van de politiegegevens die via het onderzoek in een geautomatiseerd werk worden verkregen. Dat is bijvoorbeeld mogelijk als onderzoek op afstand wordt verricht in een computer die is beveiligd met een vingerafdruk scan.

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?

Nee, het ligt niet voor de hand dat bij het onderzoek in een geautomatiseerd werk het BSN-nummer, of een ander persoonsgebonden nummer worden verwerkt.

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.

De beleidsdoelstelling waarvoor de politiegegevens verwerkt worden is de opsporing en vervolging van misdrijven waarvoor op grond van artikel 67, eerste lid, Sv voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren. De onderhavige politiegegevens hebben met elkaar gemeen dat zij kunnen bijdragen aan de waarheidsvinding en de verzameling van bewijs voor het voor de rechter brengen van verdachten voor het plegen van strafbare feiten dan wel dat zij sturingsinformatie voor het opsporingsonderzoek kunnen opleveren. De verwerking van dit soort politiegegevens vindt plaats op basis van artikel 9 van de Wet politiegegevens.

Een andere beleidsdoelstelling kan zijn om bepaalde digitale gegevens ontoegankelijk te maken. Hierbij kan het gaan om bijvoorbeeld door verdachten via geautomatiseerde weg verspreide of bewaarde gegevens die een ernstig strafbaar feit opleveren.

4. Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?

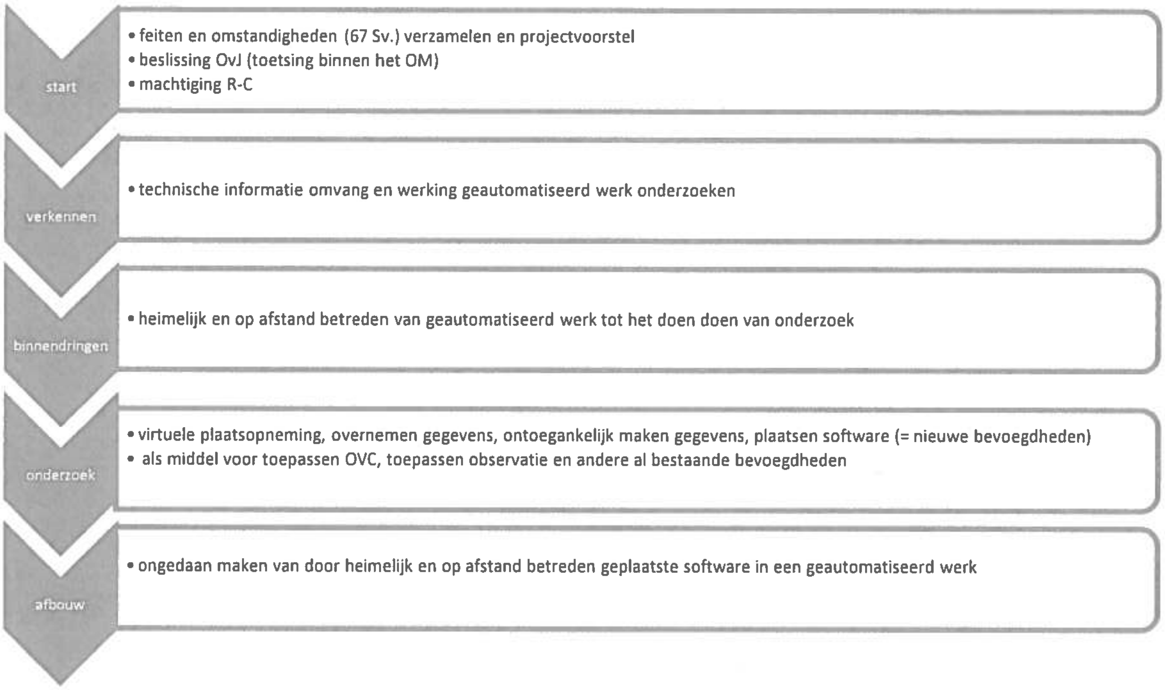
Neen. Het doel van opsporing en vervolging is juist de waarheidsvinding over strafbare feiten en de mogelijke toerekenbaarheid van die feiten aan personen. Daartoe moeten personen worden geïdentificeerd.

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

Dit wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken. Daartoe wordt voorgesteld te komen tot uitbreiding van de strafvorderlijke bevoegdheden en van een aantal strafbepalingen. De voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk voorziet in een leemte in de bestaande wettelijke bevoegdheden. De bestaande opsporingsbevoegdheden schieten in toenemende mate tekort om tegemoet te komen aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van criminaliteit waarbij gebruik wordt gemaakt van de vele mogelijkheden van ICT. Deze ontwikkelingen kunnen als volgt worden geschetst: het verbergen van de identiteit, de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken en cloud computing diensten.

Het toepassingsbereik van onderzoek in een geautomatiseerd werk, beperkt zich niet tot specifieke gevallen van computercriminaliteit, zoals computervredebreuk of het gebruik van botnets voor het platleggen van vitale infrastructuur door verstikkingsaanvallen (de zogenaamde "DDoS-aanvallen"). De bevoegdheid kan ook ten aanzien van andere misdrijven worden toegepast waarvoor op grond van artikel 67, eerste lid, Sv voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren.

Figuur 1 = algemeen proces



Het binnendringen van een geautomatiseerd werk wordt verricht door opsporingsambtenaren die niet tot het opsporingsteam behoren dat is belast met het onderzoek naar een ernstig strafbaar feit, en die door de verantwoordelijke (Korpschef en vergelijkbare verantwoordelijke bij de Koninklijke marechaussee en de bijzondere opsporingsdiensten) daartoe zijn geautoriseerd.

Voor de uitoefening van de nieuwe bevoegdheden wordt en zal gebruik gemaakt worden van nieuwe technologieën. Dit kan zowel software zijn als technische toepassingen.

II. Doeleinden/doelbinding en koppeling

1. Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?

Ja. Het doel van de bevoegdheid van onderzoek in een geautomatiseerd werk is om toegang te verkrijgen tot de gegevens die in een geautomatiseerd werk zijn of worden verwerkt ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven. Via een verbinding, zoals een intern netwerk, het internet of een Wi-Fi-verbinding, kan op afstand toegang worden verkregen tot een geautomatiseerd werk.

De voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk voorziet in een leemte in de bestaande wettelijke bevoegdheden om ernstige vormen van criminaliteit te kunnen bestrijden door onderzoek te kunnen verrichten in een geautomatiseerd werk of in een daarmee in verbinding staande gegevensdrager met het oog op de in het voorgestelde artikel 125ja, eerste lid, Sv omschreven doelen. In het bijzonder dienen de voorgestelde bevoegdheden het doel dat bestaat uit het vergaren of vorderen van gegevens die mogelijk als bewijs kunnen dienen bij de vervolging van strafbare feiten en of sturingsinformatie voor een opsporingsonderzoek kunnen opleveren.

Het onderzoek in een geautomatiseerd werk kan uitsluitend plaatsvinden met het oog op het verrichten van bepaalde onderzoekshandelingen, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het inzetten van bepaalde afzonderlijke bijzondere opsporingsbevoegdheden. De koppeling aan deze handelingen, maatregel en bevoegdheden houdt verband met het op afstand heimelijk binnendringen van een geautomatiseerd werk en betreft het volgende:

- Het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker
- Het overnemen van gegevens
- De ontoegankelijkmaking van gegevens
- Het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie
- De stelselmatige observatie.

2. Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).

Vanwege de nauwe samenhang met de bestaande bevoegdheid van de doorzoeking ter vastlegging van gegevens, zoals geregeld in artikel 125i Sv, is de voorgestelde bevoegdheid in de zevende afdeling van Titel IV ('Enige bijzondere dwangmiddelen') van het Wetboek van Strafvordering opgenomen. In de zevende afdeling is de doorzoeking ter vastlegging van gegevens geregeld. De betrokken gegevens zijn in beide gevallen dezelfde. Ook kan een geautomatiseerd werk in beslag worden genomen met het oog op het nemen van een strafrechtelijk relevante beslissing, zoals het aan de dag brengen van de waarheid. De gegevens die op dat geautomatiseerde werk zijn opgeslagen, kunnen dan worden geraadpleegd ten behoeve van de waarheidsvinding. Nieuw is dat

de gegevens worden vergaard en verwerkt via bijvoorbeeld het internet, dus op afstand en heimelijk.

Voor de regeling rond het binnendringen van het geautomatiseerde werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht. Het toepassingsbereik van onderzoek in een geautomatiseerd werk, beperkt zich niet tot specifieke gevallen van computercriminaliteit, zoals computervredebreuk of het gebruik van botnets voor het platleggen van vitale infrastructuur door verstikkingsaanvallen (de zogenaamde "DDoS-aanvallen"). De bevoegdheid kan ook ten aanzien van andere misdrijven worden toegepast waarvoor op grond van artikel 67, eerste lid, Sv voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren. Ook bij het voorbereiden en plegen van meer traditionele misdrijven is het gebruik van moderne ICT-voorzieningen een steeds belangrijker component geworden, bijvoorbeeld als het gaat om (versluierde) communicatie tussen criminelen. Het kan gaan om misdrijven als moord, handel in drugs, mensenhandel, omvangrijke milieudelicten, wapenhandel, maar ook ernstige financiële misdrijven, zoals omvangrijke ernstige fraude. De opsporingspraktijk heeft ook in die gevallen de behoefte aan de voorgestelde bevoegdheid.

3.Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?

Neen. De doeleinden blijven ongewijzigd, te weten de opsporing van ernstige misdrijven ten behoeve van de strafrechtelijke handhaving van de rechtsorde. Er is geen sprake van hergebruik van politiegegevens voor een ander doel.

4. Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het Cbp indien er geen FG is?

Is niet van toepassing in dit onderhavige wetsontwerp.

5. Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?

Is niet van toepassing in dit onderhavige wetsontwerp.

Kwaliteit

6. Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel op overheids ICT-systeem verwerkte persoonsgegevens na te gaan?

Artikel 4 van de Wet politiegegevens regelt dat de verantwoordelijke voor de politiegegevens maatregelen treft opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. De persoonsgegevens die hier worden verwerkt, worden op een forensische wijze uit het geautomatiseerde werk veiliggesteld en vastgelegd. De handelingen worden gelogd, waardoor zichtbaar en controleerbaar is hoe de gegevens zijn verkregen. Tevens worden de handelingen in een proces-verbaal vastgelegd.

De opsporingsambtenaren en de betrokken leden van het openbaar ministerie zijn zich ervan bewust van het risico dat in de eerste fases van het onderzoek onjuiste of onvolledige gegevens over het strafbare feit en over de verdachte worden verzameld. Dit kan leiden tot een verkeerde conclusie over welk geautomatiseerd werk heimelijk binnengedrongen moet worden. Dit kan geautomatiseerde werken betreffen die niets te maken hebben met de strafbare feiten die de aanleiding vormen voor het opsporingsonderzoek. Het zou bijvoorbeeld kunnen dat de betreffende geautomatiseerde werken die worden onderzocht helemaal niet in gebruik zijn bij de verdachte. Tenslotte is er het risico van bewuste identiteitsfraude en identiteitsverwisseling. Verder onderzoek kan uitwijzen dat er bijvoorbeeld sprake is van manipulatie van gegevens. Voorbeelden hiervan zijn dat er misbruik wordt gemaakt van de identiteit van een persoon of van zijn geautomatiseerd werk. Dit kan bijvoorbeeld als criminelen door hacking van het geautomatiseerde werk van een willekeurige persoon ten behoeve van hun criminele activiteiten gebruik maken van dit geautomatiseerde werk. Bedacht moet worden dat het onderzoek in een geautomatiseerde werk bedoeld is om in te zetten bij ernstige strafbare feiten en in die gevallen dat niet of net zo goed op een andere, minder invasieve wijze, gegevens over een strafbaar feit en, of de verdachte daarvan uit geautomatiseerde werken kunnen worden vergaard. Het is bij voorbaat niet geheel uit te sluiten dat op basis van onjuiste of onvolledige gegevens beslissingen worden genomen over de inzet van een bijzondere opsporingsbevoegdheid. De politie is met dat risico bekend. De voor het onderzoek in een geautomatiseerd werk te verrichten handelingen worden daarom in de praktijk in de vorm van een projectvoorbereiding door de daartoe aangewezen opsporingsambtenaren voorbereid en vervolgens aan de officier van justitie voorgelegd. Binnen het openbaar ministerie vindt een interne toetsing plaats waarna door de officier van justitie een machtiging van de rechter-commissaris wordt gevraagd. Voordat in een geautomatiseerd werk, dat in gebruik is bij een bekende of een niet bekende verdachte, daadwerkelijk wordt binnengedrongen, worden zo veel mogelijk gegevens binnen het opsporingsonderzoek vergaard die zicht geven op de werking of het gebruik van het geautomatiseerde werk. De kans dat gewerkt gaat worden op basis van onjuiste of incomplete gegevens wordt vanwege de intensieve voorbereiding met controlemomenten klein ingeschat. Het achteraf opnieuw controleren in het geautomatiseerde werk van de juistheid van de gegevens is gezien de aard van de gegevens niet mogelijk. Het gaat vaak om vluchtige gegevens. Conform artikel 4 lid 1 van de Wet politiegegevens zullen gegevens worden verbeterd of vernietigd als zij incorrect of onvolledig blijken te zijn.

Profilering

7. Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden in het kader van een om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?

Nee, de verzamelde/verwerkte politiegegevens worden in het kader van een strafrechtelijk onderzoek gebruikt ten behoeve van de opsporing van ernstige misdrijven en niet om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen.

8. Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?

Er is geen sprake van profilering. Wel kunnen de politiegegevens, die in verschillende opsporingsonderzoeken worden verwerkt, met elkaar in verband worden gebracht. Artikel 11 van de Wet politiegegevens schept de mogelijkheid om geautomatiseerd te vergelijken en in combinatie te zoeken. De gerelateerde gegevens kunnen verder worden verwerkt na instemming van een daartoe bevoegde functionaris (artikel 11, tweede lid, Wpg). Voor verdere verwerking is dus menselijke tussenkomst voorzien.

III. Betrokken instanties/systemen en verantwoordelijkheid

1. Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?

Zoals ook al is aangegeven bij de beantwoording van vraag 8 van paragraaf 2 zijn er tijdens het opsporingsproces verschillende interne en externe instanties betrokken. In de eerste plaats zijn dit de opsporingsambtenaren. In de tweede plaats is er sprake van functiescheiding, doordat de gegevens worden verzameld door andere opsporingsambtenaren, die daartoe specifiek zijn geautoriseerd, dan de opsporingsambtenaren die de gegevens verder verwerken ten behoeve van het opsporingsonderzoek naar ernstige strafbare feiten. In de tweede plaats de officier van justitie en zijn medewerkers en de rechter-commissaris, die zijn belast met de afgifte van een bevel respectievelijk een machtiging voor het onderzoek in een geautomatiseerd werk.

De veiliggestelde persoonsgegevens worden gebruikt voor de bewijsvoering en of het richting geven aan het opsporingsonderzoek. Via de onderzoekdossiers (processen-verbaal) van de politie worden politiegegevens verstrekt aan de officier van justitie en via hem aan de rechter. Deze verstrekking vindt plaats op basis van artikel 16 lid 1 onder b van de Wet politiegegevens. Deze Wet bevat regels over de verstrekking van politiegegevens aan derden, deze regels zijn van toepassing op de verzamelde en verwerkte gegevens.

2. Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?

Ja, het is in ieder stadium duidelijk wie verantwoordelijk is voor de verwerking van de politiegegevens. De Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens geven regels voor de verantwoordelijke voor de gegevensverwerking. Dit is de korpschef respectievelijk het College van procureurs-generaal. De betrokken opsporingsambtenaren, de betrokken ambtenaren van het openbaar ministerie en de zittende magistratuur zijn via opleiding en taakverdeling voldoende voorbereid op hun taken in het kader van de verwerking van persoonsgegevens. Bij of krachtens algemene maatregel ven bestuur zullen nadere eisen worden gesteld aan de opsporingsambtenaren die belast worden met de doorzoeking in geautomatiseerde werken.

3.Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?

Wie toegang heeft tot politiegegevens is uitgebreid in de Wet politiegegevens en het Besluit politiegegevens geregeld. Artikel 6 van de Wet politiegegevens regelt dat de verantwoordelijke de autorisaties regelt voor de ambtenaren die onder zijn beheer vallen voor de verwerking van politiegegevens ter uitvoering van de onderdelen van de politietaak waarmee zij zijn belast. Gezien de gevoeligheid van het binnendringen in een geautomatiseerd werk wordt aanvullend in artikel 125ja lid 6 onder c Sv geregeld dat bij of krachtens algemene maatregel van bestuur regels worden gesteld over de autorisatie en de deskundigheid van de opsporingsambtenaren die kunnen worden

belast met het verrichten van het onderzoek, bedoeld in het eerste lid van artikel 125ja Sv, en de samenwerking met andere opsporingsambtenaren. De toegang van ambtenaren van het openbaar ministerie en de zittende magistratuur tot de persoonsgegevens is niet anders dan in de normale toegang tot gegevens bij opsporing en vervolging. Dit soort onderzoeken vindt plaats in de beveiligde omgeving van de betrokken organisaties. De Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens bevatten specifieke regels voor de verstrekking van persoonsgegevens aan derden.

Deze maatregelen zijn geschreven in het belang van de opsporing en vervolging en de goede procesorde. Al het mogelijke moet worden gedaan ervoor te zorgen dat de gegevens niet in handen komen van onbevoegden.

4. Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?

Ja. Voor de opsporingsambtenaar of de persoon aan wie politiegegevens ter beschikking zijn gesteld geldt een geheimhoudingsplicht (artikel 7 Wpg). Daarvan kan uitsluitend worden afgeweken voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht, de Wet politiegegevens verstrekking toelaten en de politietaak in bijzondere gevallen tot verstrekking noodzaakt.

5. Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?

Ja. Dit is mogelijk op grond van de reeds in het voorafgaande deel aangegeven vastlegging van de opsporingshandelingen per proces-verbaal, de logging en de overige voorwaarden waaronder verwerking en uitwisseling van politiegegevens binnen strafrechtelijke onderzoeken worden verricht. De betrokkene heeft het recht op kennisneming van de politiegegevens die hem betreffen en die verwerking ondergaan (artikel 25 Wpg). Daarbij gelden echter weigeringsgronden, onder meer in het belang van de goede uitvoering van de politietaak (artikel 27, eerste lid, Wpg).

6. Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?

Ja. De verwerking van politiegegevens met het oog op de uitvoering van de politietaak is geregeld in paragraaf 2 van de Wet politiegegevens. In paragraaf 5 is het toezicht nader uitgewerkt. Het gaat hier om het uitvoeren van audits, het benoemen van privacyfunctionaris, het toezicht van het College bescherming persoonsgegevens en de benoeming van een functionaris voor de gegevensbescherming. De Wet politiegegevens biedt de mogelijkheid een bewerker aan te wijzen, de relevante bepaling van de Wet bescherming persoonsgegevens zijn dan van toepassing (artikel 4,

zesde lid, Wpg). Verwezen wordt naar de beantwoording hierboven onder vraag 3 waar wordt ingegaan op de extra maatregelen die worden genomen gezien de gevoeligheid van het binnendringen in een geautomatiseerd werk.

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?

Ja, dat is mogelijk. Artikel 17 van de Wet politiegegevens bepaalt dat politiegegevens kunnen worden verstrekt aan autoriteiten in een ander land die zijn belast met de uitvoering van de politietaak. Dit is nader uitgewerkt in het Besluit politiegegevens, waarvan artikel 5.1 regelt dat politiegegevens kunnen worden verstrekt aan autoriteiten in een ander land, die zijn belast met de uitvoering van de politietaak, voor zover dit noodzakelijk is voor de goede uitvoering van de politietaak in het desbetreffende land ingeval van de opsporing van een ernstig misdrijf of de voorkoming van een ernstig gevaar voor de openbare orde. Op grond van de Wet politiegegevens kunnen politiegegevens alleen aan een ander land worden verstrekt indien bij het ontvangende land voldoende waarborgen aanwezig zijn voor een juist gebruik van de verstrekte gegevens en voor de bescherming van de persoonlijke levenssfeer.

IV. Beveiliging en bewaring/vernietiging

1.Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging ?

Ja. Het beleid met betrekking tot gegevensbeveiliging binnen de organisaties is op orde. De verantwoordelijke is conform artikel 1 f van de Wet politiegegevens binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan. Artikel 4 onder lid 3 regelt specifiek wat de verantwoordelijke moet regelen gericht op gegevensbescherming en gegevensbeveiliging.

2. Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?

De gegevensverwerking zal niet bij een bewerker plaatsvinden, waardoor dit punt niet van toepassing is.

3. Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

Aangezien het gaat om politiegegevens en de verwerking ook binnen de verantwoordelijkheid en de randvoorwaarden van de Wet politiegegevens plaatsvindt, is dit conform geregeld. De software wordt voorafgaand aan de inzet gecertificeerd. Zo wordt zeker gesteld dat alleen onderzoekshandelingen worden verricht en gegevens worden vergaard die met het desbetreffende bevel zijn geautoriseerd. De onderzoekshandelingen worden vastgelegd (logging) om controle door de rechter achteraf mogelijk te maken.

4. Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?

Aangezien het gaat om politiegegevens en de verwerking ook binnen de verantwoordelijkheid en de randvoorwaarden van de Wet politiegegevens plaatsvindt, is dit conform geregeld.

5. Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?

De Wet politiegegevens bepaalt in paragraaf 2 de verwerking van politiegegevens met het oog op de uitvoering van de politietaak inclusief de bewaartermijnen. In beginsel worden de gegevens verwerkt voor zover nodig voor de vervulling van het doel van het opsporingsonderzoek. Daarna worden de gegevens verwijderd of gedurende een periode van een half jaar verwerkt teneinde te

bezien of zij aanleiding geven tot een nieuw opsporingsonderzoek (artikel 9, vierde lid, Wpg) . Daarna worden de verwijderde gegevens gedurende een periode van vijf jaar bewaard ten behoeve van verwerking met het oog op afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd (artikel 14, eerste lid, Wpg).

6. Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?

De Wet politiegegevens bepaalt in paragraaf 2 de verwerking van politiegegevens met het oog op de uitvoering van de politietaak inclusief de bewaartermijnen.

7. Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?

In artikel 4 van de Wet politiegegevens is vastgelegd dat de verantwoordelijke de nodige maatregelen treft opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt of dit door enige wettelijke bepaling wordt vereist. Voor de controle op de vernietiging wordt verwezen naar het antwoord op de vraag paragraaf III onder 6.

V. Transparantie en rechten van betrokkenen

Transparantie

Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?

De betrokkene kan bij de verantwoordelijke een verzoek indienen tot kennisneming van de persoonsgegevens die hem betreffen en die verwerking ondergaan (artikel 25, eerste lid, Wpg). Een dergelijk verzoek wordt afgewezen voor zover het onthouden van kennisneming noodzakelijk is in het belang van, onder meer, de uitvoering van de politietaak (artikel 27, eerste lid, Wpg). Gezien het feit dat het hier gaat om heimelijke opsporing wordt het onderzoek belemmerd indien het doel van het verwerken van de gegevens bij de betrokkenen bekend of het bekend kan gemaakt worden. De processtukken worden ook verstrekt aan de raadsman van de verdachte. Op grond van het Wetboek van Strafvordering zal gelden dat de betrokkene schriftelijk mededeling wordt gedaan van het onderzoek in het geautomatiseerde werk, conform de regeling voor de doorzoeking ter vastlegging van gegevens (artikel 125m Sv).

2. Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?

De gegevens worden niet direct verkregen van de betrokkenen.

3. Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?

De gegevens worden niet verkregen via een andere overheidsorganisatie.

Rechten van betrokkenen

4. Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?

De toestemming wordt niet gevraagd.

5. Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?

De Wet politiegegevens bepaalt in de artikelen 25, 26 en 27 de procedure voor betrokkenen ten aanzien van de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt. Een aparte regeling voor derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, om in de gelegenheid gesteld worden gesteld hun zienswijze te geven, is er niet.

6. Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?

De Wet politiegegevens kent de artikelen 28, 29, 30 en 31 waarin een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens is geregeld.